Math100B - HW #1

Jay Ser

2026.01.11

1.

By the distributive law and cancellation law, $0r = (0+0)r = 0r + 0r \implies 0r = 0$

2.

Take any $a \in \mathbb{Q}$. Then a is the root of the linear polynomial $x - a$, hence a is an algebraic number.

3.

$(x-(7+\sqrt{2}))(x-(7-\sqrt{2})) = (x-7)^2 - (\sqrt{2})^2 = x^2 - 14x + 47 \in \mathbb{Q}[x]$. By the above computation, $7+\sqrt{2}$ is a root of the polynomial $x^2 - 14x + 47$, so it is an algebraic number over $\mathbb{Q}$.

Similarly,

$$\begin{aligned}
&(x-(\sqrt{3}+\sqrt{-5}))(x-(\sqrt{3}-\sqrt{-5}))(x-(-\sqrt{3}+\sqrt{-5}))(x-(-\sqrt{3}-\sqrt{-5})) \\
=&((x-\sqrt{3})^2 - (\sqrt{-5})^2)((x+\sqrt{3})^2 - (\sqrt{-5})^2) \\
=&(x^2 - 2\sqrt{3}x + 8)(x^2 + 2\sqrt{3}x + 8) \\
=&x^4 + 16x^2 + 64 - (2\sqrt{3}x)^2 \\
=&x^4 + 4x^2 + 64
\end{aligned}$$

Clearly, $\sqrt{3}+\sqrt{-5}$ is a root of $x^4 + 4x^2 + 64 \in \mathbb{Q}[x]$, so $\sqrt{3}+\sqrt{-5}$ is an algebraic number over $\mathbb{Q}$.

4.

Take $a + b\sqrt{p}, c + d\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$.

- $(a+b\sqrt{p}) + (c+d\sqrt{p}) = (a+c) + (b+d)\sqrt{p} \in \mathbb{Z}[p]$.
- $(a+b\sqrt{p})(c+d\sqrt{p}) = (ac+bdp) + (bc+ad)\sqrt{p} \in \mathbb{Z}[p]$.

Since multiplication and addition are commutative and associative in $\mathbb{Z}$, multiplication and addition in $\mathbb{Z}[\sqrt{p}]$ are commutative and associative too. $0 + (a + b\sqrt{p}) = a + b\sqrt{p}$ so $0 \in \mathbb{Z}[\sqrt{p}]$ is the additive identity. $\forall a + b\sqrt{p} \neq 0 \in \mathbb{Z}[\sqrt{p}]$, $(a + b\sqrt{p}) + (-a + (-b)\sqrt{p}) = 0$, so every nonzero element has a nonzero identity. $1 \cdot (a+b\sqrt{p}) = a+b\sqrt{p}$, so $1 \in \mathbb{Z}[\sqrt{p}]$ is the multiplicative identity. This verifies that $\mathbb{Z}[\sqrt{p}]$ is a commutative ring.

Define the following norm function on $\mathbb{Z}[\sqrt{p}]$:

$$\lambda : \mathbb{Z}[\sqrt{p}] \to \mathbb{Z}; \quad a + b\sqrt{p} \to a^2 - pb^2$$

The following calculation shows that λ is a multiplicative function:

$$\begin{aligned}
\lambda(a + b\sqrt{p})\lambda(c + d\sqrt{p}) &= (a^2 - pb^2)(c^2 - pd^2) \\
&= a^2c^2 + p^2b^2d^2 - p(b^2c^2 + a^2d^2) \\
\lambda((a + b\sqrt{p})(c + d\sqrt{p})) &= \lambda(ac + pbd + (bc + ad)\sqrt{p}) \\
&= a^2 + 2pabcd + pb^2d^2 - p(b^2c^2 + 2abcd + a^2d^2) \\
&= a^2c^2 + p^2b^2d^2 - pb^2c^2 - pa^2d^2
\end{aligned}$$

i.e., $\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta)\, \forall \alpha, \beta \in \mathbb{Z}[\sqrt{p}]$.

Suppose $\alpha \in \mathbb{Z}[\sqrt{p}]$ is a unit. Then $\exists \beta \in \mathbb{Z}[\sqrt{p}]$ such that $\alpha\beta = 1$. Applying the norm on both sides of the equality yields

$$\lambda(\alpha)\lambda(\beta) = 1$$

Since λ maps to the integers, $\lambda(a) = \pm 1$.

Conversely, suppose $\lambda(\alpha) = \pm 1$. Write $\alpha = a + b\sqrt{p}$. Notice that $\lambda(a + b\sqrt{p}) = (a + b\sqrt{p})(a - b\sqrt{p})$. So if $\lambda(\alpha) = 1$, then $a - b\sqrt{p}$ is α's inverse; if $\lambda(\alpha) = -1$, then $b\sqrt{p} - a$ is α's inverse. This shows that $\alpha \in \mathbb{Z}[\sqrt{p}]$ is a unit $\iff \lambda(\alpha) = \pm 1$.

One can define a similar norm function on the Gaussian integers, namely

$$\lambda(a + bi) = a^2 + b^2$$

Notice that λ now maps to only the nonnegative integers with $\lambda(\alpha) = 0 \iff \alpha = 0$. Furthermore, the exact same bidirectional proof for the units in $\mathbb{Z}[i]$ follow: $a + bi \in \mathbb{Z}[i]$ is a unit $\iff \lambda(a + bi) = 1$, where one need not consider the $\lambda(\alpha) = -1$ anymore.

Specifically, $\lambda(a + bi) = a^2 + b^2 = 1 \iff a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. One concludes that the only units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

5.

First, here are some trivial calculations.

- $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}, \quad , \gamma^2 = 5 + 2\sqrt{6}$.
- The irreducible (minimal) polynomial for γ over $\mathbb{Z}$, and thus over $\mathbb{Q}$, is $x^4 - 10x^2 + 1$.
- Since γ is, well, the sum of $\sqrt{2}$ and $\sqrt{3}$, $\gamma \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $\gamma \in \mathbb{Z}[\sqrt{2}, \sqrt{3}]$. Thus $\mathbb{Z}[\gamma] \subset \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ and $\mathbb{Q}[\gamma] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

(a) $\mathbb{Q}[\gamma] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$

It must be shown that $\sqrt{2}, \sqrt{3} \in \mathbb{Q}[\gamma]$. Well, $\gamma^3 = 11\sqrt{2} + 9\sqrt{3}$, so $\sqrt{2} = 2^{-1}(\gamma^3 - 9\gamma) \in \mathbb{Q}[\gamma]$ and $\sqrt{3} = -2^{-1}(\gamma^3 - 11\gamma) \in \mathbb{Q}[\gamma]$.

(b) $\mathbb{Z}[\gamma] \subsetneq \mathbb{Z}[\sqrt{2}, \sqrt{3}]$

It must be shown that either $\sqrt{2} \notin \mathbb{Z}[\gamma]$ or $\sqrt{3} \notin \mathbb{Z}[\gamma]$. I will cheat and use ring extensions. Since $x^4 - 10x^2 + 1$ is the irreducible polynomial for γ over $\mathbb{Z}$,

$$\mathbb{Z}[\gamma] \cong \mathbb{Z}[x]/(x^4 - 10x^2 + 1)$$

This is by the First Isomorphism Theorem for rings: consider the substition homomorphism

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}[\gamma]; \quad x \to \gamma, \quad \varphi|_{\mathbb{Z}} = \mathrm{id}$$

Obviously $x^4 - 10x^2 + 1 \in \ker \varphi$, so $(x^4 - 10x^2 + 1) \subset \ker \varphi$. Conversely, suppose $f(x) \in \ker \varphi$. Dividing $f(x)$ with remainder by $x^4 - 10x^2 + 1$,

$$f(x) = (x^4 - 10x^2 + 1)q(x) + r(x)$$

where $r(x) = 0$ or $\deg r < \deg x^4 - 10x^2 + 1$. Suppose $r(x) \neq 0$. Since $x^4 - 10x^2 + 1, f(x) \in \ker \varphi$, $r(x) \in \ker \varphi$. In other words, $r(\gamma) = 0$ and $r(x)$ has degree less than $x^4 - 10x^2 + 1$. But $x^4 - 10x^2 + 1$ is the minimal polynomial that has γ as a root, which gives a contradiction. So $r(x) = 0$, and $f(x) \in (x^4 - 10x^2 + 1)$. This shows that $\ker \varphi = (x^4 - 10x^2 + 1)$, and thus $\mathbb{Z}[x]/(x^4 - 10x^2 + 1) \cong \mathbb{Z}[\gamma]$ by the First Isomorphism Theorem.

Since the irreducible polynomial for γ over $\mathbb{Z}$ is monic and has degree 4, $\{1, \gamma, \gamma^2, \gamma^3\}$ form a basis for $\mathbb{Z}[\gamma]$ over $\mathbb{Z}$ (view $\mathbb{Z}[\gamma]$ as $\mathbb{Z}[x]/(x^4 - 10x^2 + 1)$ and perform division with remainder by $x^4 - 10x^2 + 1$ in the quotient ring).

Suppose $\sqrt{2} \in \mathbb{Z}[\gamma]$. Then $\exists a_0, \ldots, a_3 \in \mathbb{Z}$ such that

$$\sqrt{2} = a_3\gamma^3 + a_2\gamma^2 + a_1\gamma + a_0$$

Substituting the calculated values for γ^2 and γ^3 yields a system of equations that can easily be solved: On the right hand side, γ^2 introduces $\sqrt{6}$ that is not present in any other term, so $a_2 = 0$. Since the left hand side doesn't have any integer part, the sum of integer terms in the left hand side must equal 0. Namely, $5a_2 + a_0 = 0 \implies a_0 = 0$. Finally, dealing with the coefficients of $\sqrt{2}$ and $\sqrt{3}$ yields the equations $11a_3 + a_1 = 1$ and $9a_3 + a_1 = 0$, which implies $2a_3 = 1$. This contradicts the fact that no integer a_3 solves $2a_2 = 1$, and thus $\sqrt{2} \neq \mathbb{Z}\gamma]$.

6.

$a \in \mathbb{Z}_n$ is a unit $\iff \exists a' \in \mathbb{Z}_n$ such that $aa' = 1 \iff \exists a' \in \mathbb{Z}$ such that $aa' = 1 \mod n$. An elementary result from number theory is that the last statement is true if and only if $(a, n) = 1$. This shows that the units in $\mathbb{Z}_n$ are equivalence classes of $\mathbb{Z}$ that are prime to n. Since prime numbers are the only integers that are coprime to every number less than it, it follows that $\mathbb{Z}_n$ is a field if and only if n is prime.

7.

$f(x) := x^2 + x + 1$ is monic, so one can divide $g(x) := x^4 + 3x^3 + x^2 + 7$ with remainder by $f(x)$:

$$x^4 + 3x^3 + x^2 + 7x + 5 = (x^2 + 2x - 2)(x^2 + x + 1) + 7x + 7$$

where $r(x) := 7x + 7$ is the remainder.

Reducing modulo n, one sees $f(x) \mid g(x)$ in $\mathbb{Z}/n\mathbb{Z} \iff r(x) = 0$ in $\mathbb{Z}/n\mathbb{Z}$. Clearly, $7x + 7 = 0 \mod n \iff n$ is a multiple of 7, i.e. $f(x) \mid g(x) \iff 7 \mid n$.

8.

Take $f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i \in F[[t]]$.

- $f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i \in F[[t]]$,
- $f(x)g(x) = \sum_{i=0}^{\infty} \sum_{j=0}^{i} a_j x^j b_{i-j} x^{i-j} = \sum_{i=0}^{\infty} \sum_{j=0}^{i} a_j b_{i-j} x^i \in F[[t]]$

That F is a field, thus equipped with commutative and associative $+$ and $\times$, allows for an easy verification that addition and multiplication are both commutative and associative in $F[[t]]$. As with the polynomial ring, it is easily verified that 0 and 1 are the additive and multiplicative identities of $F[[t]]$, respectively. Every $f(x) \in F[[t]]$ has an additive inverse, namely the polynomial whose coefficient at each index is the additive inverse in F of the corresponding coefficient in $f(x)$. This verifies that $F[[t]]$ is a commutative ring.

The following shows that $f(x) = \sum_{i=0}^{\infty} a_i x^i \in F[[t]]$ is a unit $\iff a_0 \neq 0$. Suppose $a_0 = 0$. Then clearly there is no $g(x) = \sum_{i=0}^{\infty} b_i x^i$ such that $f(x)g(x) = 1$ since the constant term is just 0. This shows that if $f(x)$ is a unit, then $a_0 \neq 0$.

Next, take any $f(x) = \sum_{i=0}^{\infty} a_i x^i \in F[[t]]$ with $a_i \neq 0$. Inductively define $g(x) = \sum_{i=0}^{\infty} b_i x^i \in F[[t]]$: For $i = 0$, $b_0 := a_0^{-1}$. For $i > 0$, suppose $b_0, \ldots, b_i$ have been defined. Then let

$$b_{i+1} := a_0^{-1}(-\sum_{k=0}^{i} a_{i-k+1} b_k)$$

With this construction, one sees via the definition of multiplication above that $f(x)g(x) = 1$: If $f(x)g(x) = \sum_{i=0}^{\infty} c_i x^i$, then $c_0 = a_0 b_0 = 1$, and for all $i > 0$,

$$b_i = a_0^{-1}(-\sum_{k=0}^{i-1} a_{i-k} b_k) \implies c_i = \sum_{k=0}^{i} a_k b_{i-k} = 0$$

** sorry for the messy indexing towards the end, got a rush of sleepiness...